

REMARKS

Claims 1-24 were originally filed in the present application.

Claims 3, 4, 6, 7, 11, 12, 14, 17, 19, 20 and 22 were previously amended.

Claims 1-24 have been rejected.

No claims have been amended herein.

No claims have been added or cancelled herein.

Claims 1-24 remain in the present application.

In a final Office Action mailed December 7, 2004, the Examiner rejected Claims 1, 3-9, 11-17, and 19-24 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,587,684, to *Hsu et al.* (hereinafter, “*Hsu*”) in view of “TIA/EIA/IS-683-A: Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems (IS683A), May 1998” (hereafter, “the IS683A reference”). The Examiner rejected Claims 2, 10 and 18 under 35 U.S.C. §103(a) as being unpatentable over the *Hsu* reference in view of the IS683A reference and further in view of U.S. Patent No. 6,609,148 to *Salo et al.* (hereafter, “*Salo*”). In a reply under 37 C.F.R. § 1.116 filed February 4, 2005, the Applicant traversed those rejections.

In an Advisory Action mailed March 9, 2005, the Examiner provided an explanation of why the Applicant’s request for reconsideration did not place the application in condition for allowance. In this submission, the Applicant respectfully traverses the rejection of the claims and the Examiner’s further assertions in the Advisory Action.

Independent Claims 9 and 1 recite the present invention from land-based and mobile perspectives, respectively. Claim 9 recites a system for secure over-the-air administration of a

wireless mobile station that converts information for transmission to the mobile station into a data burst message, converts the data burst message into a plurality of encrypted IP packets, and transmits the encrypted packets as wireless messages to the mobile station. Claim 1 recites a mobile station that receives wireless messages and converts them into IP packets, decrypts the IP packets, and converts the decrypted IP packets into a data burst message.

In contrast, the *Hsu* reference describes a system that downloads software to a digital telephone in a very different way than that employed by the Applicant's invention. The Applicant respectfully submits that even the combination of the *Hsu* reference with the teaching of the IS683A reference does not teach or suggest the invention as recited in the claims of the present application.

The *Hsu* reference teaches using hypertext-based security to establish a secure two-way client-server application layer session between a data proxy gateway server and a digital telephone. *See Hsu, col. 6, lines 51-56.* This session is established between software in the application layer of the digital telephone and software in the application layer of the data proxy gateway server. *See Hsu, Fig. 2; col. 15, lines 7-9.*

With regard to downloading control software from the server to the telephone, *Hsu* describes the server sending the software in TCP/IP data packets, whose payload data is stripped out by an interworking function (IWF) or mobile switching center (MSC) and placed into RLP/IS-95A packets for transmission to the digital telephone. *See Hsu, Fig. 2, col. 16, lines 10-17.* When the digital telephone receives the RLP/IS-95A packets, the telephone strips the payload data and sends it to software in an upper protocol layer and application layer. *See Hsu,*

col. 16, lines 18-21. That software reassembles the packet payload data and writes the executable program into non-volatile memory using file transfer protocol (FTP) software in the upper protocol layer and application layer. *See Hsu, col. 16, lines 21-26.*

Thus, the *Hsu* teaches a system in which a data proxy gateway server uses hypertext-based security techniques to encode control software for a digital telephone. The server then sends the encoded software towards the telephone in TCP/IP packets. Along the way, in an IWF or MSC, the TCP/IP packets are converted into RLP/IS-95A packets for wireless transmission to the telephone. Upon receiving the packets, physical layer software in the telephone sends the packet data to application layer software. One skilled in the art would recognize that these packets would be reassembled before decryption, since they were encrypted in the server before TCP/IP packetization. After decryption, the *Hsu* system writes the decrypted software to non-volatile memory.

The Applicant traverses the Examiner's assertion that the Applicant's invention as recited in the claims is obvious in view of the combination of the *Hsu* reference and the IS683A reference. In the land-based portion of the *Hsu* system, the information for transmission to the mobile station is encoded first, in a secure application layer session, and then converted by physical layer software into TCP/IP packets. Furthermore, an Internet server with no knowledge of the IS-95A/IS-683A wireless communication protocol performs these actions. As such, the Applicant respectfully submits that even in view of the teaching of the IS-683A reference, one of ordinary skill in the art would not have been led to invert the protocol layers in the *Hsu* Internet server by first converting the information into a physical layer data burst message according to

the IS-683A reference, followed by encrypting the data burst message in a plurality of IP packets, as recited in Claim 9.

Similarly, regarding Claim 1, the *Hsu* reference teaches using physical layer software to extract data from IS-95A packets, then using software in upper protocol layers to reassemble the data and decrypt it. Here too, the person of ordinary skill would not have been motivated by the IS-683A reference to reverse the functionality of the *Hsu* protocol layer stack and perform application level decryption before reassembly of a physical layer data burst message, as recited in Claim 1.

Regarding Claim 9, which recites a system that sends information to a mobile station, in the final Office Action mailed December 7, 2004, the Examiner asserted that *Hsu* discloses “a data burst message protocol controller/IWF-MSC (Fig. 1) capable of receiving and converting [information for download to a mobile station] into at least one message (col. 6, lines 6-54).” *Page 6, lines 10-12.* The Examiner reiterated this assertion in the Advisory Action, mailed March 9, 2005, and cited more specifically to column 6, lines 21-25 and 43-45, of the *Hsu* reference. *Continuation Sheet, lines 11-12.* The Applicant respectfully submits that the Examiner mischaracterizes the teaching of the *Hsu* reference.

The first cited passage states: “As shown in FIG. 1, the system includes an Interworking Function Unit (IWF) 18, configured for establishing a 2-way communication link with the digital telephone according to a prescribed network layer protocol, such as TCP/IP protocol.” *Hsu, col. 6, lines 21-25.* The second cited passage states: “Hence, the IWF 18 recovers the TCP/IP

messages from the CDMA data packets transported according to radio link protocol (RLP) . . . ”

Hsu, col. 6, lines 43-45.

The cited passages describe converting RLP/IS95A packets to and from TCP/IP packets in messages sent between a mobile telephone and an Internet server. As discussed above, during the transmission of control software to a mobile telephone, such packets are pieces of a secure application layer message that were encrypted before being packetized. In sharp contrast, Claim 9 recites a system for administration of a wireless mobile station that converts information into a data burst message before converting it into a plurality of encrypted IP packets and transmitting the packets as wireless messages to the mobile station.

In rejecting Claim 9, the Examiner stated that *Hsu* “does not explicitly disclose the data burst message protocol controller capable of converting said decrypted IP packets to at least one *data burst message*.” *Office Action mailed Dec. 7, 2004, page 6, lines 19-21 (emphasis in the original)*. However, because the IS683A standard teaches that messages are sent in the fields of Data Burst Messages, the Examiner asserted “it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a data burst protocol controller to convert the IP packets to data burst messages.” *Office Action mailed Dec. 7, 2004, page 6, line 22, to page 7, line 2*. The Applicant respectfully submits that the Examiner has misunderstood the language of Claim 9.

Claim 9 recites a data burst message protocol controller capable of converting information to be sent to a mobile station into a data burst message. Claim 9 further recites an encryption controller capable of converting the data burst message into a plurality of encrypted

IP packets. Thus, Claim 9 does not recite “a data burst protocol controller to convert the IP packets to data burst messages,” which the Examiner asserts would be obvious from the combination of the *Hsu* reference and the IS683A reference. As such, the Examiner has not established a *prima facie* case of obviousness against Claim 9.

Referring to *Hsu*, column 13, lines 35-61, the Examiner asserted in the Advisory Action mailed March 9, 2005, that *Hsu* “uses the I683A protocol by encapsulating OTS/data burst messages in the TCP/IP packets via an interpreter interface.” The Applicants respectfully submit that the Examiner mischaracterizes the teaching of the *Hsu* reference.

In the passage relied upon by the Examiner, the *Hsu* reference describes its IS-95A interface as delivering OTA messages according to IS-683. *See Hsu, col. 13, lines 34-36.* A microbrowser in the *Hsu* system uses a URL-encoding format (e.g., device://file/parameters) to communicate with Internet servers. *See Hsu, col. 13, lines 26-30.* Because of this, *Hsu* describes an interpreter residing in one of the protocol layers above the physical IS-95A layer to convert the URL format messages from the microbrowser into IS-683 format messages for transmission over the wireless link. *See Hsu, col. 13, lines 36-39.* Upon receiving a message in the byte-oriented format specified under IS-683, the interpreter converts the message into the character-oriented URL format used by the microbrowser. *See Hsu, col. 13, lines 39-60.* For example, the byte-oriented message shown in Table 1 of the *Hsu* reference is encoded in the interpreter as the character string: “HTTP://provision server address/OTASP_MSG_TYPE + NUM_BLOCKS + BLOCK_ID + BLOCK_LEN + PARAM_DATA”. *See Hsu, col. 13, lines 42-58.*

The Applicant respectfully submits that the cited passage does not teach the encapsulation of OTA/data burst messages into TCP/IP packets, as asserted by the Examiner. Instead, it teaches the conversion of byte-oriented IS-683 messages into character strings for use by the *Hsu* microbrowser.

SUMMARY

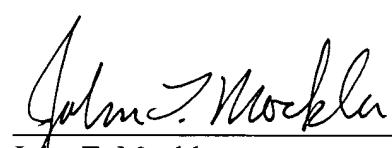
For the reasons given above, the Applicants respectfully request reconsideration and allowance of pending claims and that this Application be passed to issue. If any outstanding issues remain, or if the Examiner has any further suggestions for expediting allowance of this Application, the Applicants respectfully invite the Examiner to contact the undersigned at the telephone number indicated below or at *jmockler@davismunck.com*.

The Commissioner is hereby authorized to charge any additional fees connected with this communication or credit any overpayment to Deposit Account No. 50-0208.

Respectfully submitted,
DAVIS MUNCK, P.C.

Date: 29 April 2005

P.O. Drawer 800889
Dallas, Texas 75380
Phone: (972) 628-3600
Fax: (972) 628-3616
E-mail: *jmockler@davismunck.com*


John T. Mockler
Registration No. 39,775